January 2019

2019's Key Tech Trend for Capital Markets? That's Private

By Monica Summerville, Head of FinTech and European Research, TABB Group

There is a Gordian Knot that needs to be cut when it comes to financial firms being able to leverage their data fully in the face of increasing data privacy rules – and an innovative technology approach enabling data pseudonymization (bonus points for pronouncing it correctly) may just be the thing to cut through. TABB Group believes the rise of data privacy-focused solutions offering technology approaches to achieving compliance, while also enabling firms to leverage their data for competitive advantage, will be a key IT theme within capital markets this year. Oh, and happy Data Privacy Day!

> "The question is no longer whether we need a federal law to protect consumers' privacy. The question is what shape that law should take."
>
> *– U.S. Senator John Thune, Chairman, Commerce Committee*

In May 2018, European citizens experienced a step-change in regulating how their private data is handled and used by companies around the globe due to the General Data Protection Regulation (GDPR) taking effect. The rest of the world is already or soon -will be following suit, especially in the wake of the data misuse scandals embroiling some of the world's biggest tech companies. For example, in January 2019, Google was fined €50 million for violating GDPR, marking the first major penalty brought against a U.S. technology giant since the regulations took effect and potentially foreshadowing greater scrutiny of tech firms in Europe.

A prominent example of the global trend to tighten laws around data privacy is the California Consumer Privacy Act, but nearly 120 countries and independent jurisdictions/territories have privacy legislation in place and almost 40 more have pending bills. The belief that this trend is growing is reflected by increased investment. In fact, Crunchbase reported nearly one-third more funding rounds by privacy start-ups in 2018 than 2017. AngelList, which follows start-up trends, picked up on this and has highlighted several start-ups benefiting from this increased

investment in data privacy solutions including: Purism (privacy-centric computers), BigID (applying ML for privacy) and Canopy (founded by Spotify-alums, offering a recommendations engine that doesn't collect user data).

Data sovereignty and privacy restrictions make it challenging to create a single view of data across borders or business lines and to leverage data for innovation. Conflict is likely to arise between legal, compliance and business lines when it comes to data use and sharing – that is, between data privacy protection and dynamic uses of data. Data sharing with third parties or even among internal business entities across geographies can be challenging or even impossible without disclosing personally identifiable information (PII) using traditional data privacy approaches.

With the financial services industry among the most highly regulated in the world and always looking for a competitive edge in achieving profit and alpha, solutions that can help in driving customer engagement are highly appealing. However, the recent global data privacy and sovereignty laws have the power to stop a financial firm from leveraging its valuable data resources by placing restrictions on common use cases for data, including:

1. Sharing and transfer of data across jurisdictions or to the cloud for cross marketing, support, etc.
2. Holistic client analysis using data from across business functions.
3. Open innovation through data sharing, leveraging the fintech ecosystem and secure Multi-Party Computing (MPC).

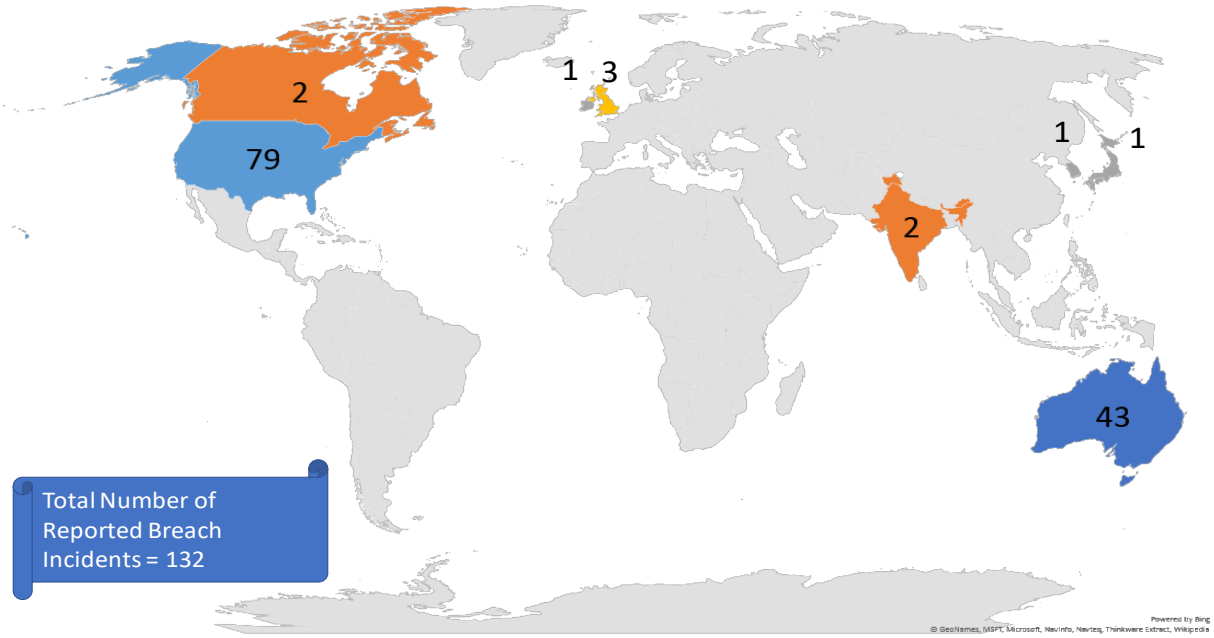
Data Privacy Restrictions Take a Step-Change with GDPR

GDPR was a step-change in data privacy because it fundamentally changed the rules on how to collect data and what you could do with it. It applies to all data collected about EU-located individuals that can directly or indirectly be used to identify them. The penalties for non-compliance are so severe that there have been reports of firms choosing to delete massive stores of data due to concerns over the legality of keeping this data.

The public is very aware and wary of how companies are using and protecting its data. They have good reason to be concerned about lax data protection. In the first half of 2018 alone there were over 130 reported data breaches within the financial services sector, which

impacted two million data records across eight countries (see Exhibit 1). Meanwhile with compliance systems playing catch up with changes in digital technology offerings, it is no surprise many people wonder whether their data privacy is being respected.

Exhibit 1: Total Number of Reported Data Breach Incidents Globally in Financial Services – 1H 2018



Source: TABB Group

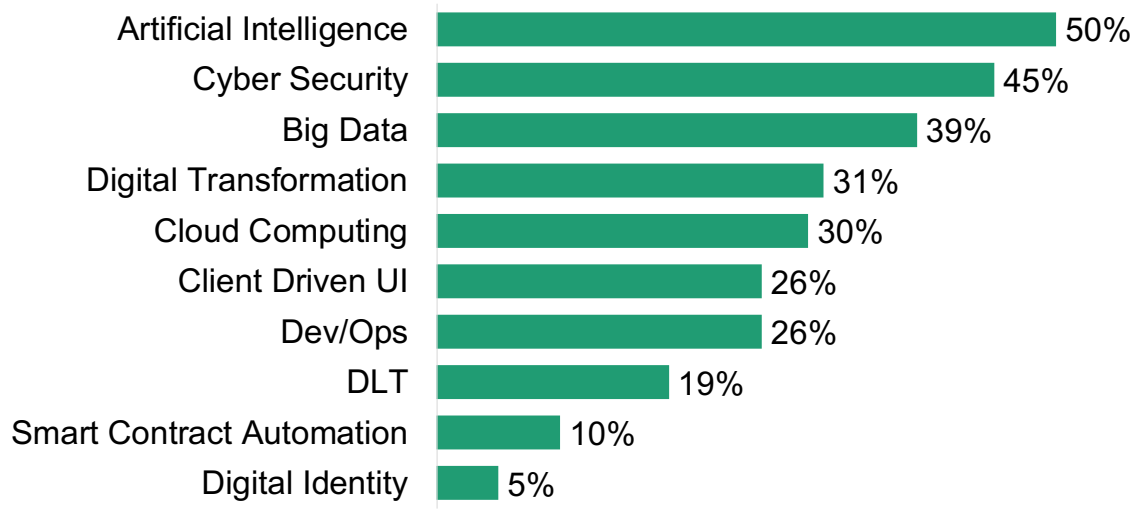
This desire by lawmakers and the public to put more controls around data privacy comes at the same time that financial institutions are increasingly looking to their data as a source of competitive advantage. Financial entities are working eagerly to resolve challenges with data governance at an enterprise level in order to support advanced data analytics. These analytics provide enhanced business insights which are increasingly powered by artificial intelligence (AI). AI, of course, depends on massive data sets, comprising structured and unstructured data, to feed its underlying models, including data sets that may include personally identifying data (PID).

Vast Data Stores Needed to Feed the AI Machine

Firms in the capital markets space are embracing AI, ranking it a top fintech priority for 2019, according to results of a TABB Group survey conducted across buy-side, sell-side, banks and

exchanges in November 2018. Of the 100+ senior executives surveyed, 50% listed AI as one of their top three initiatives (see Exhibit 2).

Exhibit 2: Top Capital Markets Priorities – November 2018

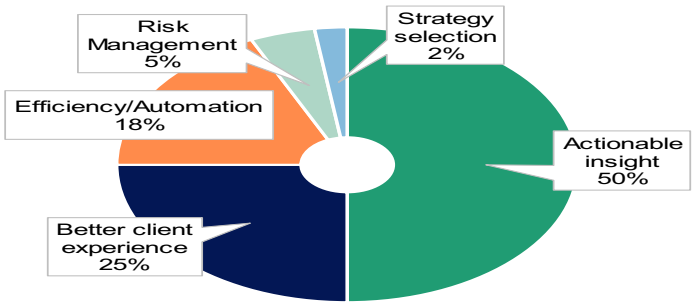


Note: Respondents chose their top 3

Source: TABB Group

The top benefits expected to be obtained from leveraging AI, according to the same research, is that of actionable insight and better client experience (see Exhibit 3). In terms of relative importance, achieving insight into strategies, whether corporate, investment or customer, surpassed the efficiencies and cost reduction to which AI could contribute by a large margin.

Exhibit 3: The Primary Benefit Expected from Incorporating AI/Machine Learning Application



Source: TABB Group

Much of this effort, however, will require the use of client data from across the enterprise. For example, a prominent use case identified in the TABB Group report "Enhanced Bankers – The Impact of AI" (April 2018) centered on the analysis of client and prospect information held within a customer relationship management (CRM) system to enhance the customer experience and increase sales by isolating past buying behavior in order to predict future purchases.

TABB Group found that most firms of all types and sizes are allocating precious budget to the development of AI and machine learning (ML) to achieve a better understanding of their clients, and therefore their businesses. Two-thirds of financial services firms further expect their budgets to be increased over the next 12 months, according to TABB Group research. But while this demonstrates a clear commitment to enhancing their business, budget alone won't make it happen. Obstacles abound for financial services organizations looking to leverage customer data for analytics or commercialization.

No General Consent

Under most new privacy regulations, customers must actively opt in to allow their PII even to be stored; negative or general consent is no longer acceptable to permit the use or analysis of customer information. Gaining retrospective consent may mean contracts need to be re-papered to achieve and reflect positive consent, but the consent may only be targeted to a specific purpose; certain data may need to be segregated from data stored in other areas of the company, impeding an enterprise-wide view of the business. As anyone who has gone through such an exercise can attest, this can become a multi-year endeavor.

Penalties for non-compliance can be severe. In addition to massive fines – under GDPR, up to €20 million or 4% of global turnover, whichever is greater – regulators can use injunctions to stop the processing or analysis of data immediately and order the deletion of data except for limited legal use, effectively bringing business to a halt. The risk to client relationships and a firm's reputation for violating legal and privacy requirements could be devastating.

Business Strategy vs. Compliance

The ability to analyse data to achieve holistic insights about customers, based on data drawn from across the enterprise and beyond, is invaluable to any company. With few exceptions, every company is now a data company. Long established financial services workflows and business models are being disrupted and innovated by fintech start-ups across a range of financial services activities, in areas spanning the full range of services, from asset management (e.g. quantitative trading, robo-investing) to trading (e.g. pre-trade analytics, low/high touch trading, all-to-all trading) to custody (e.g. digital assets). Data privacy solutions developed in response to previous regulation, however, has never had to address the requirements of the latest wave of privacy regulations.

In the runup to GDPR, many companies were unaware that data collected under broad-based consent would no longer be legal after the regulation's go-live date. In panic responses, some firms chose to irreversibly anonymise or simply delete data entirely to avoid the risk of liability. Some industry estimates suggest that nearly 20% of B2B companies have deleted data due to concerns over legality and compliance. In some instances, decades' worth of customer loyalty data has been deleted.

The increasing liabilities and costs of compliance under new regulations no longer are just costs of doing business – regulators can shut down businesses. In some organizations, big data projects are being cancelled due to confusion around data policies or the inability to meet compliance requirements, leading to loss of revenue and competitive advantage. Some firms are attempting to comply by anonymizing data or keeping it in silos with targeted consent. And while these approaches may be technically compliant, the data loses its value for analytics and business intelligence.

Transforming Data from a Liability to an Asset

Where should companies start on the road to compliance and to maximizing the value of their data? First, they need to identify the sensitive personal data in their organizations and determine where it resides across the network. Then they need to transform and store the

data in a compliant, yet accessible format. After all, the new data privacy laws are designed to ensure that the data used by a company to feed analytics and AI is processed in strict compliance with the new regulations.

Many firms still rely heavily on consent when leveraging customer data as their main method of permitting re-use of data under GDRP. However, as this approach gives individuals distinct granular choice and ongoing control over their consent, the re-use of data sourced this way can be limited. Alternatively, to fulfill GDPR's requirement that data used "does not relate to an identifiable natural person or to data rendered anonymous in such a way that the data subject is no longer identifiable," other firms simply anonymized their data, a one-way process that limits the usefulness of the data for all but very high-level data aggregation and analysis

However, GDPR itself offered a new concept for European data law called "pseudonymization." Article 3 of GDPR defines data pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." The "new" part of this approach is that the data is separated from direct identifiers in a way that means any linkage is simply not possible without referring to separate information held elsewhere.

Data processed this way is still subject to GDPR, but there are some significant relaxations in terms of use. For example, processing the data in this way allows for the use of data under the "legitimate interest" provisions of GDPR. This contrasts with data collected due to a regulatory obligation, consent or as part of a contract, which is not available to be repurposed for unrelated analytics and AI.

GDPR supports pseudonymization throughout its text including in Articles 6 (4) e, Article 11 (2), Article 25 (1), Article 32 (1) (a), Article 34, Article 40 (2) (d), and Article 89 (1). These Articles deal with a range of important issues including permitting the processing of personal data for uses other than those for which it was originally collected, exemptions from complying with an individual's rights to access, rectify, or erase their personal data, ensuring security of processing personal data, notification in case of data breach, and use of data for historical and statistical purposes.

Dynamic pseudonymization is seen as superior to other approaches such as anonymization and tokenization, as, in addition to irreversibly degrading the insight value of the data these methods also allow the possibility of illegally identifying subjects as multiple large databases are analyzed together (the so-called “mosaic effect”). Dynamic pseudonymization also allows for valuable controlled re-linking of the data by authorized personnel.

Certainly, these are simple definitions of complex techniques, but it is good to know that at least one pseudonymization technology is certified by Europrivacy.org, the European certification scheme co-funded by the European Commission (EC), as a compliant data masking method for GDPR. If a technique can address the extremely high standard of GDPR, it is likely to comply and meet the requirements of the 100 or more global jurisdictions mandating data protection.

The awareness of dynamic pseudonymization seems to be as rare as solutions providers who support it. One fintech making a splash in this area is Anonos, a new data risk management, security and privacy company with a strong financial services pedigree. Its solution is certified by EuroPrivacy.org as complying with legal and technical requirements for pseudonymizing data under GDPR and its founders were also behind FTEN, which helped revolutionize risk-management by making real-time intraday risk calculations possible. FTEN was sold to NASDAQ in 2010.

PrivacyTech Is a Thing

The growth of innovative technology solutions for privacy, for example those supporting the pseudonymization of data, will be a key trend this year. TABB Group has found that the focus on data privacy globally is increasing from both a customer and regulator perspective to a point that funding interest in this space experienced a marked increase in 2018. The appeal for financial services firms in these data-obsessed times is clear: once a company takes steps to identify and pseudonymize its customer PII in way that protects their customers’ privacy, complies with regulations and retains the business value inherent in the data, it can then take the next step of maximizing this value using AI and analytics. This means satisfying both its legal obligations and its business demands.

Data privacy regulation, led by the EU's GDPR, is just beginning to have an impact on financial services businesses and has already influenced global rule makers. Firms need to act now to address those compliance requirements and protect themselves in a way that not only keeps regulators satisfied, but also opens a world of possibilities.

To learn more about developments in FinTech, please contact TABB Group.

▲

To see comments and join the discussion, visit FORUM.

Not yet a member of TabbFORUM? Please complete a free registration: Sign-up for TabbFORUM

HITACHI
Inspire the Next

Distributed by Hitachi Vantara